AO 106 (Rev. 06/09) Application for a Search Warrant

UNDER SEAL

UNITED STATES DISTRICT COURT

for the

Eastern District of Virginia

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Apple iPhone, Model A1660
IMEI: 355311082116148

Case No. 1:17sw763

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*
See Attachment A (incorporated by reference).

located in the Eastern District of Virginia, there is now concealed *(identify the person or describe the property to be seized)*:
See Attachment B (incorporated by reference).

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
21 U.S.C. § § 841(a)(1) & 846	Conspiracy to Distribute Controlled Substances (Crack/Cocaine)

The application is based on these facts:
See attached affidavit of Jonathan C. Boller, ATF Special Agent

- ☐ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Jonathan Boller
Applicant's signature

Jonathan C. Boller, ATF Special Agent
Printed name and title

Sworn to before me and signed in my presence.

Date: 11/7/2017

/s/ JFA
John F. Anderson
United States Magistrate Judge
Judge's signature

City and state: Alexandria, Virginia

The Hon. John F. Anderson U.S. Magistrate Judge
Printed name and title

ATTACHMENT A

The property to be searched is listed below and currently located at the ATF Falls Church II Evidence Locker at 7799 Leesburg Pike, Falls Church, Virginia 22043:

Device #	Make	Model	Identifier
1	Apple	A1660 iPhone	355311082116148

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Device described in Attachment A that relate to violations of Title 21, United States Code, Sections 841(a)(1) and 846 and involve Malik ALLEN, including:

   a. Any conversations, whether through text messages or other applications, where Malik ALLEN discusses controlled substances;

   b. lists of customers and related identifying information;

   c. types, amounts, and prices of drugs trafficked as well as dates, places, and amounts of specific transactions;

   d. any information related to sources of drugs (including names, addresses, phone numbers, or any other identifying information);

   e. any information recording Malik ALLEN's schedule or travel from December 2016 to the date phones came into law enforcement's possession; and

   f. all bank records, checks, credit card bills, account information, and other financial records.

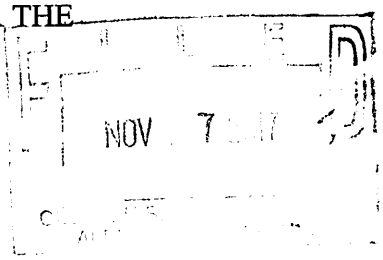
2. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

UNDER SEAL

IN THE UNITED STATES DISTRICT COURT FOR THE

EASTERN DISTRICT OF VIRGINIA

Alexandria Division



IN THE MATTER OF THE SEARCH OF Apple iPhone, Model A1660 IMEI: 355311082116148 CURRENTLY LOCATED AT ATF Falls Church II Evidence Locker 7799 Leesburg Pike, Falls Church, Virginia 22043	**Under Seal** 1:17-sw-763

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Jonathan C. Boller, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—electronic devices—which are currently in law enforcement possession, and the extraction from those devices of electronically stored information described in Attachment B.

2. I have been a Special Agent with the Bureau of Alcohol, Tobacco, Firearms and Explosives ("ATF") since 2016. I have experience investigating narcotics and firearms trafficking offenses.

3. As an ATF Special Agent, I have investigated and assisted in the investigation of narcotics and firearms traffickers. I have previously participated in investigations, which resulted in the arrest and conviction of narcotics and firearms traffickers. I have also become familiar with the methods and techniques associated with the distribution of narcotics and how

drug trafficking organizations work. From 2014 to 2016, I served as a Special Agent with the United States Secret Service, where I received specialized training including certification in the Basic Investigation of Computer and Electronic Crimes Program.

4. Based on my training and experience, and the experience of other law enforcement officers, in investigating narcotics and the distribution of narcotics while armed, I know that it is common for individuals engaged in this activity to use telephonic communications, both cellular (to include voice and text messages) and hard line, to further their criminal activities. I know that "smart" phones play an integral role in the daily lives of individuals engaging in narcotics trafficking and that these individuals use cellular telephones to exchange information with customers and/or source(s) of supply through text messaging, instant messaging, and telephone conversations. I also know that it is common for narcotics traffickers to use multiple "smart" phones to communicate with co-conspirators in order to compartmentalize their illegal activity and avoid detection by law enforcement. Further, I know it is common for narcotics traffickers to change their phones and phone numbers in order to avoid detection by law enforcement.

5. The facts and information contained in this affidavit are based upon my personal knowledge, information obtained from federal and state law enforcement officers, and information obtained from interviews and analysis of reports.

6. This affidavit contains information necessary to support probable cause and is not intended to include each and every fact and matter observed by me or known to the government.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

7. The property to be searched is listed below (hereinafter referred to as "the Device"). The Device is currently located in the ATF Falls Church II evidence locker, which is

located at 7799 Leesburg Pike, Falls Church, Virginia 22043, which is within the Eastern District of Virginia. The Device is listed in the below table. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

Device #	Make	Model	Identifier
1	Apple	A1660 iPhone	IMEI: 355311082116148

PROBABLE CAUSE

A. Background on the Investigation

1. In February 2017, a cooperating source ("CI-1") reported to the Prince William County Police Department that Co-Conspirator 1 was a narcotics distributor. CI-1 is a member of the Imperial Gangster Blood gang. CI-1 will be referred to in the masculine gender, regardless of CI-1's true gender. CI-1 has been convicted of two felonies, including robbery and a probation violation. He was arrested in December of 2016, in Prince George's County, Maryland, for possessing a stolen firearm as a convicted felon and possession of controlled substances. CI-1 originally cooperated because he hoped to receive a lesser sentence. Based on CI-1's cooperation, Prince George's County dismissed his charges. CI-1 continues to cooperate because he is being compensated. CI-1 also hopes to be relocated.

2. Based on this information and because Co-Conspirator 1 is a known member of the Imperial Gangster Blood gang, ATF opened an investigation into Co-Conspirator 1.

B. Purchase of 224 grams of Marijuana and 15 grams of Cocaine from Co-Conspirator 1

8. On October 14, 2017, CI-1 was socializing with Co-Conspirator 1 at ATF request. While present with Co-Conspirator 1, CI-1 learned that a high-level IGB member that CI-1 knew as "LEEK" (later identified as Malik Jovan ALLEN) would be coming to purchase illegal drugs from Co-Conspirator 1. CI-1 became aware of this information by being present in the room when Co-Conspirator 1 received a series of Facetime calls and voice calls from ALLEN.

9. CI-1 told me the iCloud account that ALLEN used to Facetime call Co-Conspirator 1 was "realgzzassociation@icloud.com." However, CI-1 stated he was not sure how it was spelled. CI-1 then told me about the pending drug sale. After being contacted, I traveled to a location within the Eastern District of Virginia where Co-Conspirator 1 is known to reside and sell illegal drugs.

10. At a later date, CI-1 provided a link to ALLEN's Facebook page, which showed that ALLEN was affiliated with a record label named "Real Geez Association". CI-1 stated that after seeing this, he recognized that to be the same way it was spelled in the iCloud account, without the spaces.

11. CI-1 then sent me two "Live" images showing Co-Conspirator 1 preparing Cocaine and Marijuana for sale. Within these images was a large plastic bag that appeared to contain two smaller bags. One of the smaller bags appeared to be white in color, while the second appeared to be green in color. Visible in the background was a scale, a white plastic bottle which CI-1 stated contained "cut" to dilute Cocaine, and a heat sealer. Also visible within these images is Malik ALLEN, standing within several feet of Co-Conspirator 1, with a large amount of U.S. Currency on a nearby countertop.

12. I then observed Malik ALLEN exit the building and enter a silver Cadillac DTS sedan bearing a Virginia vehicle registration plate. I followed ALLEN in this vehicle from the area of Co-Conspirator 1's residence onto Interstate 95 South to the Quantico, Virginia area. A short time later, I contacted the Virginia State Police and informed them of the events that had transpired.

13. A short time later, the Virginia State Police located ALLEN's vehicle and initiated a traffic stop for a motor vehicle violation. After being informed he was being detained, ALLEN fled the traffic stop in his vehicle. After a high-speed pursuit, Virginia State Police apprehended ALLEN, arresting him for several state level offenses. The Virginia State Police recovered approximately 224 grams of suspected Marijuana and 15 grams of suspected Cocaine from ALLEN's vehicle, as well as the Device, believed to be ALLEN's phone. The Device was seized from the vehicle and stored in evidence by the Virginia State Police. The phone is a Black Apple iPhone model A1660 IMEI: 355311082116148.

14. On October 23, 2017, the Virginia State Police turned over custody of the Device to the ATF. The Device is currently in storage at 7799 Leesburg Pike, Falls Church, Virginia 22043, Virginia, which is located within the Eastern District of Virginia. In my training and experience, I know that the Device have been stored in a manner in which the contents are, to the extent material to this investigation, in substantially the same state as they were when the Device first came into the possession of the ATF.

15. After a search warrant is obtained for the Device, ATF or FBI will begin the search of the Device within the Eastern District of Virginia. If ATF or FBI cannot complete the search then agents will send the Device to a private company that specializes in data extraction from Apple iPhones and other electronics. This private company will either (a) unlock the

Device and then return the Device to the ATF or FBI office located in the Eastern District of Virginia, where the actual analysis of the contents of the Device will take place or (b) unlock the Device and create a forensic image of the Device, and then return the Device to the ATF or FBI office located in the Eastern District of Virginia, where the actual analysis of the contents of the Device will take place.

TECHNICAL TERMS

16. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. *Wireless telephone*: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. *Digital camera*: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. *Portable media player*: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. *GPS*: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated

"GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. *PDA*: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include GPS technology for determining the location of the device.

f. *Internet*: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international

borders, even when the devices communicating with each other are in the same state.

17. Based on my training, experience, and research, and from consulting the manufacturer's advertisements and product technical specifications available online at http://www.apple.com/iphone/, I know that the Device has capabilities that allow them to serve as the following: a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on smart phones can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

18. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

19. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

20. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

21. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose

many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

22. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premise. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

23. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,

Jonathan Boller

Jonathan Boller
Special Agent
Bureau of Alcohol, Tobacco, Firearms and Explosives

Subscribed and sworn to before me on November 7, 2017:

/s/ JFA
John F. Anderson
United States Magistrate Judge

The Honorable John F. Anderson
United States Magistrate Judge

ATTACHMENT A

The property to be searched is listed below and currently located at the ATF Falls Church II Evidence Locker at 7799 Leesburg Pike, Falls Church, Virginia 22043:

Device #	Make	Model	Identifier
1	Apple	A1660 iPhone	355311082116148

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Device described in Attachment A that relate to violations of Title 21, United States Code, Sections 841(a)(1) and 846 and involve Malik ALLEN, including:

   a. Any conversations, whether through text messages or other applications, where Malik ALLEN discusses controlled substances;

   b. lists of customers and related identifying information;

   c. types, amounts, and prices of drugs trafficked as well as dates, places, and amounts of specific transactions;

   d. any information related to sources of drugs (including names, addresses, phone numbers, or any other identifying information);

   e. any information recording Malik ALLEN's schedule or travel from December 2016 to the date phones came into law enforcement's possession; and

   f. all bank records, checks, credit card bills, account information, and other financial records.

2. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.